SNORT

What is SNORT ?

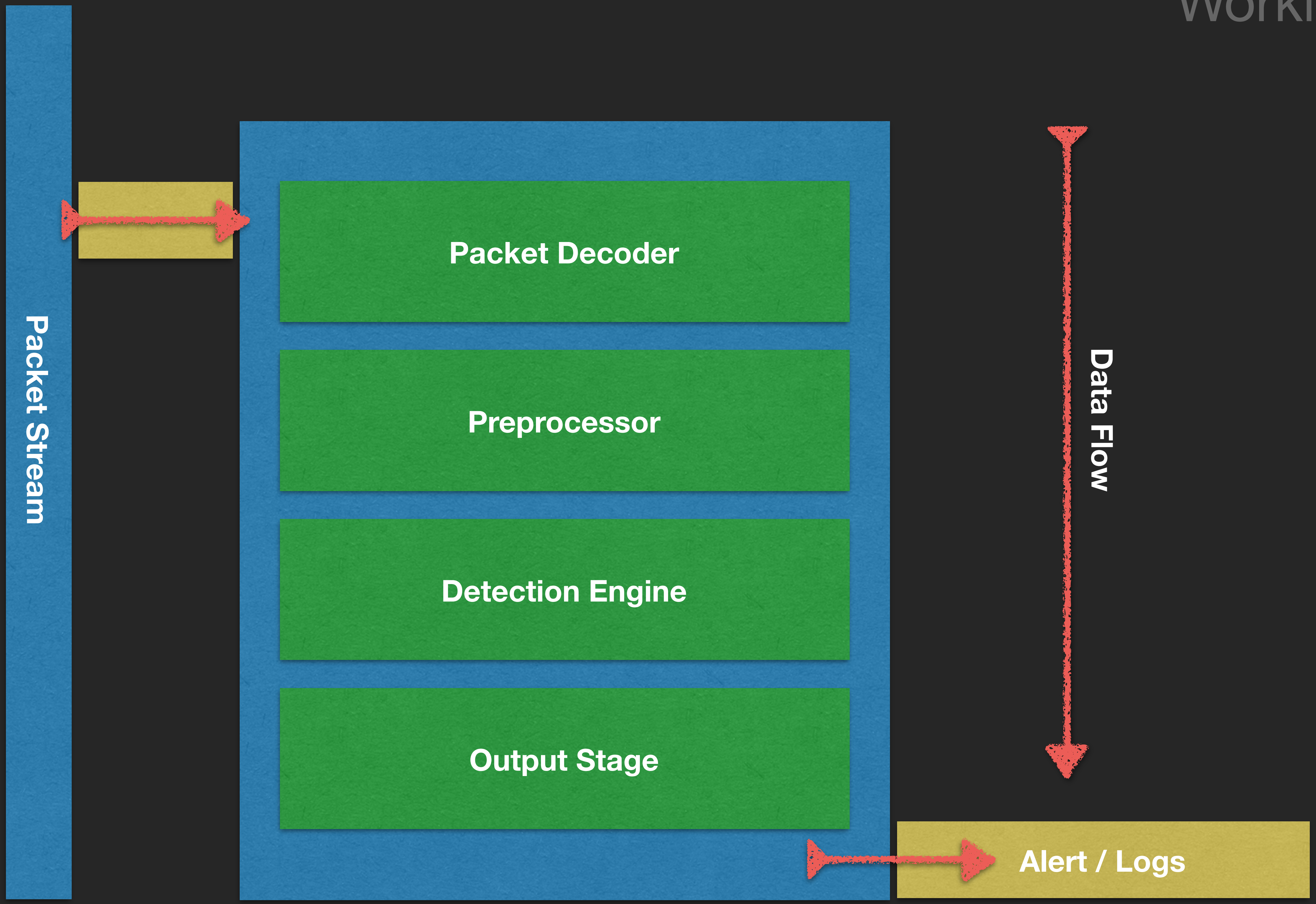
SNORT is an open source IDS and IPS by CISCO , it is capable of performing real time traffic analysis and packet logging on the IP network.

Three supported modes

- Sniffer mode
- Packet Logger mode
- NIDS

SNORT

Working



Basic Rule Structure

```
[action] [protocol] [sourceIP] [sourceport] -> [destIP] [destport] ( [Rule options] )
```

THANK YOU!